



This document is scheduled to be published in the Federal Register on 11/02/2011 and available online at <http://federalregister.gov/a/2011-28406>.

9110-06

## **DEPARTMENT OF HOMELAND SECURITY**

Office of the Secretary

[Docket No. DHS-2011-0102]

Privacy Act of 1974; Department of Homeland Security U.S. Customs and Border Protection DHS/CBP-003 Credit/Debit Card Data System of Records

**AGENCY:** Privacy Office, DHS.

**ACTION:** Notice of Privacy Act system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974 the Department of Homeland Security proposes to establish a new Department of Homeland Security system of records notice titled “Department of Homeland Security/ U.S Customs and Border Protection – 003 Credit/Debit Card Data System of Records.” This system allows U.S. Customs and Border Protection to collect, use, and maintain records related to any credit and debit card transactions with it has with individuals. Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, concurrent with this system of records elsewhere in the Federal Register. This newly established system will be included in the Department of Homeland Security’s inventory of record systems.

**DATES:** Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

**ADDRESSES:** You may submit comments, identified by docket number DHS-2011-0102 by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 703-483-2999.
- Mail: Mary Ellen Callahan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.
- Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to <http://www.regulations.gov>, including any personal information provided.
- Docket: For access to the docket to read background documents or comments received go to <http://www.regulations.gov>.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact: Laurence E. Castelli (202-325-0280), Privacy Officer, Office of International Trade, U.S. Customs and Border Protection, Mint Annex, 799 Ninth Street, NW, Washington, DC 20229. For privacy issues please contact: Mary Ellen Callahan (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

## **SUPPLEMENTARY INFORMATION:**

### **I. Background**

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) proposes to establish a new DHS system of records notice titled, “DHS/CBP-003 Credit/Debit Card Data System of Records.”

This system collects, uses, and maintains records related to any credit and

debit card transactions with CBP. CBP is providing notice to the public regarding the collection, use, and dissemination of any credit and debit card transaction information provided to CBP. Many programs administered by CBP require an individual or business to provide payment for various purposes, including services, applications, fees, and duties, among others. As CBP expands methods of payment, many of these transactions will permit use of credit and debit cards, which will require the collection of the card data, disseminating that data to process the transaction, and maintaining the data for recordkeeping purposes. Information from this system will be shared with the Department of Treasury, banks, and credit and debit card processors as necessary. The data will not be used for law enforcement or intelligence purposes unless the individual's underlying transaction becomes associated with a law enforcement or intelligence action.

The purpose of this system is to provide payment processing and recordkeeping of credit and debit card transactions with CBP. Authority for maintenance of this system is given by The Homeland Security Act of 2002, Public Law 107-296; 5 U.S.C. § 301; 8 U.S.C. § 1101, et seq.; 19 U.S.C. § 1, et seq.; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), (Pub. L. 110-53); and the Travel Promotion Act (Pub. L. 111-145).

This newly established system will allow CBP to collect credit and/or debit card payment information from individuals providing payment to CBP for services, applications, fees, duties, and other official activities. Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed

to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. All routine uses proposed are compatible with the purpose for which the information was collected and CBP's mission.

Consistent with DHS's information sharing mission, information stored in the Credit/Debit Card Data system of records may be shared with other DHS components, as well as appropriate federal, state, local, foreign, or international or tribal government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

Additionally, the Department of Homeland Security is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, concurrent with this system of records elsewhere in the Federal Register. DHS is not exempting any data in the system regarding an individual's credit or debit card transaction. This system, however, may contain records or information pertaining to the accounting of disclosures made from this system to other law enforcement or intelligence agencies (federal, state, local, foreign, international or tribal) in accordance with the published routine uses or statutory basis for disclosure under 5 U.S.C. § 552a(b). For the accounting of these disclosures only, in accordance with 5 U.S.C. §§ 552a (j)(2), and (k)(2), DHS will claim exemptions for these records or information.

## II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. Below is the description of the U.S. Customs and Border Protection DHS/CBP-003 Credit/Debit Card Data system of records.

In accordance with 5 U.S.C. § 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

**System of Records**

Department of Homeland Security (DHS)/U.S. Customs and Border Protection  
(CBP) - 003

**System name:**

DHS/CBP – 003 Credit/Debit Card Data System

**Security classification:**

Unclassified

**System location:**

Records are maintained in the Automated Commercial System at the CBP Headquarters in Washington, D.C. and field offices.

**Categories of individuals covered by the system:**

Categories of individuals covered by this system include any individuals that provide credit or debit card information as a means of payment to CBP.

**Categories of records in the system:**

Categories of records in this system include:

- Individual's Name;
- Address;
- Billing Name;
- Billing Address;
- Credit or Debit Card Number;
- Card Expiration Date;

- Charge Amount;
- Authorization Number; and
- Tracking numbers.

**Authority for maintenance of the system:**

The Homeland Security Act of 2002, Public Law 107-296; 5 U.S.C. § 301; 8 U.S.C. § 1101, et seq.; 19 U.S.C. § 1, et seq.; Section 711 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), (Pub. L. 110-53); and the Travel Promotion Act (Pub. L. 111-145).

**Purpose(s):**

The purpose of this system is to provide payment processing and recordkeeping of credit and debit card transactions with CBP.

**Routine uses of records maintained in the system, including categories of users and the purposes of such uses:**

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

A. To the Department of Justice (including United States Attorney Offices) or other federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is relevant and necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. any employee of DHS in his/her official capacity;
3. any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee; or
4. the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised;
2. The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or



programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

G. To an appropriate federal, state, local, foreign, international or tribal law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To the Department of Treasury's Pay.gov, banks, and credit and debit card processors, for payment processing and payment reconciliation purposes.

**Disclosure to consumer reporting agencies:**

None.

**Policies and practices for storing, retrieving, accessing, retaining, and**

**disposing of records in the system:****Storage:**

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD-ROM.

**Retrievability:**

Records may be retrieved by any of the data elements listed in categories of records, above.

**Safeguards:**

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

**Retention and disposal:**

Payment information will be maintained in this system for nine months in an active state to reconcile accounts and six years and three months in an archived state in conformance with NARA General Schedule 6 Item 1 Financial Records management requirements. The nine month active status is necessary to handle reconciliation issues (including chargeback requests and retrievals). CBP must respond to these issues within 10 to 15 days or lose the payment.

**System Manager and address:**

Director, Office of Automated Systems, U.S. Customs and Border  
Protection Headquarters, 1300 Pennsylvania Avenue, NW., Washington, DC  
20229.

**Notification procedure:**

The Secretary of Homeland Security has exempted portions of this system from the notification, access, and amendment procedures of the Privacy Act because it is a law enforcement system. However, CBP will consider individual requests to determine whether or not information may be released. Thus, Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Headquarters or component's FOIA Officer, whose contact information can be found at <http://www.dhs.gov/foia> under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0655, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for

this purpose from the Director, Disclosure and FOIA, <http://www.dhs.gov> or 1-866-431-0486. In addition you should provide the following:

- An explanation of why you believe the Department would have information on you,
- Identify which component(s) of the Department you believe may have the information about you,
- Specify when you believe the records would have been created,
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records,
- If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

**Record access procedures:**

See “Notification procedure” above.

**Contesting record procedures:**

See “Notification procedure” above.

**Record source categories:**

Records are obtained from individuals directly in the course of collecting payment for various purposes, including services, applications, fees, and duties, among others.

**Exemptions claimed for the system:**

No exemption shall be asserted with respect to information maintained in the system as it relates to data submitted by or on behalf of a person who provided payment information. Information in the system may be shared with law enforcement and/or intelligence agencies pursuant to the above routine uses. The Privacy Act requires DHS maintain an accounting of the disclosures made pursuant to all routines uses. Disclosing the fact that a law enforcement or intelligence agencies has sought particular records may affect ongoing law enforcement or intelligence activity. As such, pursuant to 5 U.S.C. § § 552 a (j)(2) and (k)(2), DHS will claim exemption from (c)(3), (d), (e)(8), and (g) of the Privacy Act of 1974, as amended, as is necessary and appropriate to protect this information.

Dated: October 3, 2011

Mary Ellen Callahan

Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2011-28406 Filed 11/01/2011 at 8:45 am; Publication Date:

11/02/2011]